

CLAIM AMENDMENTS

- 1 1. (Currently Amended) A method for facilitating Internet security protocol (IPsec)
2 based communications through a device that employs address translation in a
3 telecommunications network, the method comprising the steps of:
4 receiving a first electronic message from a first node, wherein:
5 the first node is associated with a first network address;
6 the first electronic message is based on IPsec;
7 the first electronic message is associated with a first identifier;
8 the first identifier is a first IPsec Security Parameter Index (SPI);
9 the first identifier is generated by the first node; and
10 the first electronic message is addressed to a second network address;
11 the device generating a value based on the first identifier and a specified scheme,
12 wherein the specified scheme is a computer-implemented operation that is
13 known to both the device that employs address translation and a second node;
14 sending the first electronic message to [[a]] the second node based on the second
15 network address, wherein the first electronic message includes a particular
16 network address that is associated with the device instead of the first network
17 address;
18 receiving a second electronic message from the second node, wherein:
19 the second electronic message is based on IPsec;
20 the second electronic message is addressed to the particular network address;
21 the second electronic message is associated with a second identifier that is
22 different than the first identifier; and
23 the second identifier is a second IPsec SPI; and
24 the second identifier is generated, based on the first identifier and the specified
25 scheme, by the second node;
26 the device determining whether the second electronic message is directed to the first
27 node based on the value and the second identifier; and

28 sending the second electronic message to the first node at the first network address
29 when the second electronic message is determined to be directed to the first
30 node.

1 2. (Currently Amended) A method as recited in claim 1, further comprising the steps of:
2 receiving a third electronic message from a third node, wherein:
3 the third node is associated with a third network address;
4 the third electronic message is based on IPsec;
5 the third electronic message is associated with a third identifier;
6 the third identifier is a third IPsec SPI; and
7 the third identifier is generated by the third node; and
8 the third electronic message is addressed to the second network address;
9 the device generating an additional value based on the third identifier and the
10 specified scheme;
11 sending the third electronic message to the second node based on the second network
12 address, wherein the first electronic message includes the particular network
13 address that is associated with the device instead of the third network address;
14 receiving, after sending the first electronic message and the third electronic message
15 to the second node, the second electronic message from the second node;
16 wherein:
17 the second electronic message is based on IPsec;
18 the second electronic message is addressed to the third network address;
19 the second electronic message is associated with the second identifier that is
20 different than the first identifier and the third identifier; and
21 the second identifier is generated, based on the third identifier and the
22 specified scheme, by the second node;
23 the device determining whether the second electronic message is directed to the third
24 node based on the additional value and the second identifier; and
25 when the second electronic message is determined to be directed to the third node,
26 sending the second electronic message to the third node at the third network
27 address.

1 3. (Cancelled)

1 4. (Previously Presented) A method as recited in claim 1, wherein the specified scheme
2 is selected from the group consisting of a first scheme that produces a fixed length
3 output, a second scheme that includes a hash algorithm, and a third scheme that
4 includes a Message Digest 5 one-way hash function.

1 5. (Cancelled)

1 6. (Cancelled)

1 7. (Cancelled)

1 8. (Cancelled)

1 9. (Previously Presented) A method as recited in claim 1, wherein:
2 the value is a hash value;
3 the second identifier is based at least in part on the hash value;
4 the hash value is comprised of a first plurality of bytes;
5 the second identifier is comprised of a second plurality of bytes;
6 a last pair of bytes of the second plurality of bytes is a first pair of bytes of the first
7 plurality of bytes; and
8 the step of determining whether the second electronic message is directed to the first
9 node further comprises the steps of:
10 comparing the last pair of bytes of the second identifier to the first pair of
11 bytes of the hash value; and
12 when the last pair of bytes of the second identifier match the first pair of bytes
13 of the hash value, determining that the second electronic message is
14 directed to the first node.

1 10. (Currently Amended) A method as recited in claim 1, wherein:
2 the first node is an IPsec originator node;
3 the second node is an IPsec responder node;

4 the first identifier is a first IPsec security parameter index;
5 the second identifier is a second IPsec security parameter index;
6 the device employs a feature selected from the group consisting of network address
7 translation (NAT), dynamic address NAT, and network address port
8 translation (NAPT);
9 and the method further comprises the steps of:
10 creating and storing a mapping between the value and the first IPsec SPI;
11 security parameter index;
12 creating an association between the value and the first IPsec SPI; identifier;
13 and
14 storing the association in a translation table.

1 11. (Previously Presented) A method as recited in claim 1, wherein the first electronic
2 message and the second electronic message are both based on an IPsec feature
3 selected from the group consisting of IPsec tunnel mode and IPsec Encapsulation
4 Security Payload.

1 12. (Cancelled)

1 13. (Cancelled)

1 14. (Cancelled)

1 15. (Cancelled)

1 16. (Previously Presented) A method as recited in claim 1, further comprising the steps
2 of:
3 when the second electronic message is determined to be directed to the first node,
4 creating an association between the first network address and the second
5 identifier;
6 storing the association in a table;

7 receiving a third electronic message from the second node, wherein the third
8 electronic message is based on IPsec and is associated with the second
9 identifier; and
10 determining that the third electronic message is directed to the first node based on the
11 association.

1 17. (Cancelled)

1 18. (Currently Amended) A method as recited in claim 1, further comprising the steps of:
2 receiving a third electronic from the second node, wherein:

3 the third electronic message is based on IPsec;
4 the third electronic message is addressed to the specified network address;
5 the third electronic message is associated with a third identifier that is
6 different than both the first identifier and the second identifier;
7 the third identifier is a third IPsec SPI; and
8 the third identifier is generated, based on the first identifier and the specified
9 scheme, by the second node;

10 the device determining whether the third electronic message is directed to the first
11 node based on the value and the third identifier; and
12 when the third electronic message is determined to be directed to the first node,
13 sending the third electronic message to the first node at the first network
14 address.

1 19. (Previously Presented) A method as recited in claim 1, wherein the step of the device
2 generating the value is performed before the step of receiving the second electronic
3 message.

1 20. (Previously Presented) A method as recited in claim 1, wherein the step of the device
2 generating the value is performed after the step of receiving the second electronic
3 message.

1 21. (Cancelled)

- 1 22. (Cancelled)
- 1 23. (Cancelled)
- 1 24. (Currently Amended) A method for facilitating Internet security protocol (IPsec)
2 based communications through a device that employs address translation in a
3 telecommunications network, the method comprising the steps of:
4 receiving a first electronic message from a first node, wherein:
5 the first node is associated with a first network address;
6 the first electronic message is based on IPsec;
7 the first electronic message is associated with a first identifier;
8 the first identifier is a first IPsec Security Parameter Index (SPI);
9 the first identifier is generated by the first node based on a second identifier
10 and a specified scheme;
11 the specified scheme is a computer-implemented operation that is known to
12 both the device that employs address translation and the first node;
13 the second identifier is a second IPsec SPI;
14 the first identifier is different than the second identifier; and
15 the first electronic message is addressed to a second network address;
16 sending the first electronic message to a second node based on the second network
17 address, wherein the first electronic message includes a particular network
18 address that is associated with the device instead of the first network address;
19 receiving a second electronic message from the second node, wherein:
20 the second electronic message is based on IPsec;
21 the second electronic message is address to the particular network address;
22 the second electronic message is associated with the second identifier; and
23 the second identifier is generated by the second node;
24 the device generating a value based on the second identifier and the specified scheme;
25 the device determining whether the second electronic message is directed to the first
26 node based on the value and the first identifier; and

27 sending the second electronic message to the first node at the first network address
28 when the second electronic message is determined to be directed to the first
29 node.

- 1 25. (Currently Amended) An apparatus for facilitating Internet security protocol (IPsec)
2 based communications with a device that employs address translation in a
3 telecommunications network, the apparatus comprising:
4 a processor; and
5 one or more stored sequences of instructions which, when executed by the processor,
6 cause the processor to carry out the steps of:
7 generating a value based on both a first identifier that is associated with a first node
8 and a specified scheme, wherein:
9 the first identifier is generated by the first node[[,]];
10 the first identifier is a first IPsec Security Parameter Index (SPI); and
11 the specified scheme is a computer-implemented operation that is known to
12 both the device that employs address translation and the first node;
13 the apparatus generating a second identifier based on the value, wherein the second
14 identifier is a second IPsec SPI; and the specified scheme;
15 receiving, from the device that employs address translation, a first electronic message
16 that originates from the first node, wherein:
17 the first electronic message is based on IPsec;
18 the first electronic message is associated with the first identifier;
19 the first electronic message includes a particular network address that is
20 associated with the apparatus instead of a first network address that is
21 associated with the first node; and
22 the first electronic message is addressed to a second network address that is
23 associated with the second node;
24 in response to receiving the first electronic message, generating a second electronic
25 message to the first node, wherein:
26 the second electronic message is based on IPsec;
27 the second electronic message is associated with the second identifier; and

28 the second electronic message is addressed to the particular network address;
29 sending the second electronic message to the device that employs address translation
30 at the particular network address;
31 wherein the device determines whether the second electronic message is directed to the
32 first node based on the second identifier and the value that is generated by the
33 device based on the first identifier and the specified scheme; and
34 wherein the device sends the second electronic message to the first node at the first
35 network address when the device determines that the second electronic
36 message is directed to the first node.

1 26. (Cancelled)

1 27. (Cancelled)

1 28. (Currently Amended) An apparatus as recited in claim 25, wherein the value is a hash
2 value, ~~the first identifier is a first IPsec Security Parameter Index (SPI), the second~~
3 ~~identifier is a second IPsec SPI~~, and the instructions for generating the second IPsec
4 SPI further comprises one or more stored sequences of instructions which, when
5 executed by the processor, cause the process to carry out the step of generating, prior
6 to receiving the first electronic message, the second IPsec SPI based on the hash
7 value.

1 29. (Currently Amended) An apparatus as recited in claim 25, wherein the value is a hash
2 value, ~~the first identifier is a first IPsec Security Parameter Index (SPI), the second~~
3 ~~identifier is a second IPsec SPI~~, the first IPsec SPI is a first randomly generated fixed
4 length value and the instructions for generating the second IPsec SPI further
5 comprises one or more stored sequences of instructions which, when executed by the
6 processor, cause the process to carry out the step of generating the second IPsec SPI
7 based on at least a first portion of the hash value and a second portion of a second
8 randomly generated fixed length value.

1 30. (Previously Presented) An apparatus for facilitating Internet security protocol (IPsec)
2 based communications through a router that employs network address translation in a
3 telecommunications network, the apparatus comprising:
4 a processor; and
5 one or more stored sequences of instructions which, when executed by the processor,
6 cause the processor to carry out the steps of:
7 receiving a first electronic message from a first IPsec originator node, wherein:
8 the first IPsec originator node is associated with a first network address;
9 the first electronic message is secured using IPsec;
10 the first electronic message is associated with a first security parameter index
11 (SPI);
12 the first SPI is generated by the first IPsec originator node; and
13 the first electronic message is addressed to a third network address;
14 the router generating a first hash value based on the first SPI and a hash algorithm;
15 sending the first electronic message to an IPsec responder node based on the third
16 network address, wherein the first electronic message includes a particular
17 network address that is associated with the router instead of the first network
18 address;
19 receiving a second electronic message from a second IPsec originator node, wherein:
20 the second IPsec originator node is associated with a second network address;
21 the second electronic message is secured using IPsec;
22 the second electronic message is associated with a second SPI;
23 the second SPI is generated by the second IPsec originator node; and
24 the second electronic message is address to the third network address;
25 the router generating a second hash value based on the second SPI and the hash
26 algorithm;
27 sending the second electronic message to the IPsec responder node based on the third
28 network address, wherein the second electronic message includes the
29 particular network address that is associated with the router instead of the
30 second network address;

31 after sending the first electronic message and the second electronic message to the
32 IPsec responder node, receiving a third electronic message from the IPsec
33 responder node, wherein:
34 the third electronic message is secured using IPsec;
35 the third electronic message is associated with a third SPI that is different than
36 the first SPI and the second SPI;
37 the third electronic message is addressed to the particular network address;
38 the third SPI is generated by the IPsec responder node based at least in part on
39 the hash algorithm;
40 the router determining whether the third electronic message is directed to the first
41 IPsec originator node based on the first hash value and the third SPI;
42 when the third electronic message is determined to be directed to the first IPsec
43 originator node, sending the third electronic message to the first IPsec
44 originator node at the first network address;
45 determining whether the third electronic message is directed to the second IPsec
46 originator node based on the second hash value and the third SPI; and
47 when the third electronic message is determined to be directed to the second IPsec
48 originator node, sending the third electronic message to the second IPsec
49 originator node at the second network address.

1 31. (Previously Presented) An apparatus as recited in claim 30, wherein the first electronic
2 message is based on IPsec tunnel mode and IPsec Encapsulating Security Payload
3 (ESP), the second electronic message is based on IPsec tunnel mode and IPsec ESP,
4 and the hash algorithm is a Message Digest 5 one-way hash function.

1 32. (Currently Amended) A computer-readable medium carrying one or more sequences
2 of instructions for facilitating Internet security protocol (IPsec) based communications
3 through a device that employs address translation in a telecommunications network,
4 which instructions, when executed by one or more processors, cause the one or more
5 processors to carry out the steps of:
6 receiving a first electronic message from a first node, wherein:

7 the first node is associated with a first address;
8 the first electronic message is based on IPsec;
9 the first electronic message is associated with a first identifier;
10 the first identifier is a first IPsec Security Parameter Index (SPI);
11 the first identifier is generated by the first node; and
12 the first electronic message is addressed to a second network address;
13 the device generating a value based on the first identifier and a specified scheme,
14 wherein the specified scheme is a computer-implemented operation that is
15 known to both the device that employs address translation and a second node;
16 sending the first electronic message to [[a]] the second node based on the second
17 network address, wherein the first electronic message includes a particular
18 network address that is associated with the device instead of the first network
19 address;
20 receiving a second electronic message from the second node, wherein:
21 the second electronic message is based on IPsec[[:]];
22 the second electronic message is addressed to the particular network address;
23 the second electronic message is associated with a second identifier that is
24 different than the first identifier;
25 the second identifier is a second IPsec SPI; and
26 the second identifier is generated, based on the first identifier and the specified
27 scheme, by the second node;
28 the device determining whether the second electronic message is directed to the first
29 node based on the value and the second identifier; and
30 sending the second electronic message to the first node at the first network address
31 when the second electronic message is determined to be directed to the first
32 node.

- 1 33. (Currently Amended) An apparatus for facilitating Internet security protocol
2 (IPsec) based communications while employing address translation in a
3 telecommunications network, comprising:
4 a processor; and

5 one or more stored sequences of instructions which, when executed by the processor,
6 cause the processor to carry out the steps of:
7 receiving a first electronic message from a first node, wherein:
8 the first node is associated with a first network address;
9 the first electronic message is based on IPsec;
10 the first electronic message is associated with a first identifier
11 the first identifier is a first IPsec Security Parameter Index (SPI);
12 the first identifier is generated by the first node based on a second identifier
13 and a specified scheme;
14 the specified scheme is a computer-implemented operation that is known to
15 both the device that employs address translation and the first node;
16 the second identifier is a second IPsec SPI;
17 the first identifier is different than the second identifier; and
18 the first electronic message is addressed to a second network address;
19 sending the first electronic message to a second node based on the second network
20 address, wherein the first electronic message includes a particular network
21 address that is associated with the apparatus instead of the first network
22 address;
23 receiving a second electronic message from the second node, wherein:
24 the second electronic message is based on IPsec;
25 the second electronic message is address to the particular network address;
26 the second electronic message is associated with the second identifier; and
27 the second identifier is generated by the second node;
28 generating a value based on the second identifier and the specified scheme;
29 determining whether the second electronic message is directed to the first node based
30 on the value and the first identifier; and
31 sending the second electronic message to the first node at the first network address
32 when the second electronic message is determined to be directed to the first
33 node.

1 34. (Cancelled)

1 35. (Currently Amended) An apparatus for facilitating Internet security protocol (IPsec)
2 based communications while employing address translation in a telecommunications
3 network, the apparatus comprising:
4 means for receiving a first electronic message from a first node, wherein:
5 the first node is associated with a first network address;
6 the first electronic message is based on IPsec;
7 the first electronic message is associated with a first identifier;
8 the first identifier is a first IPsec Security Parameter Index (SPI);
9 the first identifier is generated by the first node; and
10 the first electronic message is addressed to a second network address;
11 means for generating a value based on the first identifier and a specified scheme,
12 wherein the specified scheme is a computer-implemented operation that is
13 known to both the device that employs address translation and a second node;
14 means for sending the first electronic message to [[a]] the second node based on the
15 second network address, wherein the first electronic message includes a
16 particular network address that is associated with the apparatus instead of the
17 first network address;
18 means for receiving a second electronic message from the second node, wherein:
19 the second electronic message is based on IPsec;
20 the second electronic message is addressed to the particular network address;
21 the second electronic message is associated with a second identifier that is
22 different than the first identifier; and
23 the second identifier is a second IPsec SPI; and
24 the second identifier is generated, based on the first identifier and the specified
25 scheme, by the second node;
26 means for determining whether the second electronic message is directed to the first
27 node based on the value and the second identifier; and
28 means for sending the second electronic message to the first node at the first network
29 address when the second electronic message is determined to be directed to
30 the first node.

1 36. (Currently Amended) An apparatus as recited in claim 35, further comprising:
2 means for receiving a third electronic message from a third node, wherein:
3 the third node is associated with a third network address;
4 the third electronic message is based on IPsec;
5 the third electronic message is associated with a third identifier;
6 the third identifier is a third IPsec SPI; and
7 the third identifier is generated by the third node; and
8 the third electronic message is addressed to the second network address;
9 means for generating an additional value based on the third identifier and the
10 specified scheme;
11 means for sending the third electronic message to the second node based on the
12 second network address, wherein the first electronic message includes the
13 particular network address that is associated with the apparatus instead of the
14 third network address;
15 means for receiving, after sending the first electronic message and the third electronic
16 message to the second node, the second electronic message from the second
17 node;
18 wherein:
19 the second electronic message is based on IPsec;
20 the second electronic message is addressed to the third network address;
21 the second electronic message is associated with the second identifier that is
22 different than the first identifier and the third identifier; and
23 the second identifier is generated, based on the third identifier and the
24 specified scheme, by the second node;
25 means for determining whether the second electronic message is directed to the third
26 node based on the additional value and the second identifier; and
27 means for sending the second electronic message to the third node at the third
28 network address, when the second electronic message is determined to be
29 directed to the third node.

- 1 37. (Currently Amended) An apparatus as recited in claim 35, wherein the specified
2 scheme is selected from the group consisting of a first scheme that produces a fixed
3 length output, a second scheme that includes a hash algorithm, and a third scheme that
4 includes a Message Digest 39 5 one-way hash function.
- 1 38. (Previously Presented) An apparatus as recited in claim 35, wherein:
2 the value is a hash value;
3 the second identifier is based at least in part on the hash value;
4 the hash value is comprised of a first plurality of bytes;
5 the second identifier is comprised of a second plurality of bytes;
6 a last pair of bytes of the second plurality of bytes is a first pair of bytes of the first
7 plurality of bytes; and
8 the means for determining whether the second electronic message is directed to the
9 first node further comprises:
10 means for comparing the last pair of bytes of the second identifier to the first
11 pair of bytes of the hash value; and
12 means for determining that the second electronic message is directed to the
13 first node, when the last pair of bytes of the second identifier match the
14 first pair of bytes of the hash value.
- 1 39. (Currently Amended) An apparatus as recited in claim 35, wherein:
2 the first node is an IPsec originator node;
3 the second node is an IPsec responder node;
4 ~~the first identifier is a first IPsec security parameter index;~~
5 ~~the second identifier is a second IPsec security parameter index;~~
6 the apparatus employs a feature selected from the group consisting of network address
7 translation (NAT), dynamic address NAT, and network address port translation
8 (NAPT);
9 and the apparatus further comprises:
10 means for creating and storing a mapping between the value and the first IPsec
11 SPI; security parameter index;

12 means for creating an association between the value and the first IPsec SPI;
13 identifier; and
14 means for storing the association in a translation table.

- 1 40. (Previously Presented) An apparatus as recited in claim 35, wherein the first
2 electronic message and the second electronic message are both based on an IPsec
3 feature selected from the group consisting of IPsec tunnel mode and IPsec
4 Encapsulation Security Payload.
- 1 41. (Previously Presented) An apparatus as recited in claim 35, further comprising:
2 means for creating an association between the first network address and the second
3 identifier, when the second electronic message is determined to be directed to
4 the first node;
5 means for storing the association in a table;
6 means for receiving a third electronic message from the second node, wherein the
7 third electronic message is based on IPsec and is associated with the second
8 identifier; and
9 means for determining that the third electronic message is directed to the first node
10 based on the association.
- 1 42. (Currently Amended) An apparatus as recited in claim 35, further comprising:
2 means for receiving a third electronic from the second node, wherein:
3 the third electronic message is based on IPsec;
4 the third electronic message is addressed to the specified network address;
5 the third electronic message is associated with a third identifier that is
6 different than both the first identifier and the second identifier;
7 the third identifier is a third IPsec SPI; and
8 the third identifier is generated, based on the first identifier and the specified
9 scheme, by the second node;
10 means for determining whether the third electronic message is directed to the first
11 node based on the value and the third identifier; and

12 means for sending the third electronic message to the first node at the first network
13 address, when the third electronic message is determined to be directed to the
14 first node.

1 43. (Previously Presented) An apparatus as recited in claim 35, wherein the value is
2 generated before the second electronic message is received.

1 44. (Previously Presented) An apparatus as recited in claim 35, wherein the value is
2 generated after the second electronic message is received.

1 45. (Currently Amended) An apparatus for facilitating Internet security protocol (IPsec)
2 based communications while employing address translation in a telecommunications
3 network, comprising:

4 a processor; and

5 one or more stored sequences of instructions which, when executed by the processor,
6 cause the processor to carry out the steps of:

7 receiving a first electronic message from a first node, wherein:

8 the first node is associated with a first network address;

9 the first electronic message is based on IPsec;

10 the first electronic message is associated with a first identifier;

11 the first identifier is generated by the first node; and

12 the first electronic message is addressed to a second network address;

13 generating a value based on the first identifier and a specified scheme, wherein the
14 specified scheme is a computer-implemented operation that is known to both
15 the device that employs address translation and a second node;

16 sending the first electronic message to [[a]] the second node based on the second
17 network address, wherein the first electronic message includes a particular
18 network address that is associated with the apparatus instead of the first
19 network address;

20 receiving a second electronic message from the second node, wherein:

21 the second electronic message is based on IPsec;

22 the second electronic message is addressed to the particular network address;

23 the second electronic message is associated with a second identifier that is
24 different than the first identifier; and
25 the second identifier is a second IPsec SPI; and
26 the second identifier is generated, based on the first identifier and the specified
27 scheme, by the second node;
28 determining whether the second electronic message is directed to the first node based
29 on the value and the second identifier; and
30 sending the second electronic message to the first node at the first network address
31 when the second electronic message is determined to be directed to the first
32 node.

1 46. (Currently Amended) An apparatus as recited in claim 45, further comprising one or
2 more stored instructions which, when executed by the processor, cause the processor
3 to carry out the steps of:
4 receiving a third electronic message from a third node, wherein:
5 the third node is associated with a third network address;
6 the third electronic message is based on IPsec;
7 the third electronic message is associated with a third identifier;
8 the third identifier is a third IPsec SPI; and
9 the third identifier is generated by the third node; and
10 the third electronic message is addressed to the second network address;
11 generating an additional value based on the third identifier and the specified scheme;
12 sending the third electronic message to the second node based on the second network
13 address, wherein the first electronic message includes the particular network
14 address that is associated with the apparatus instead of the third network
15 address;
16 receiving, after sending the first electronic message and the third electronic message
17 to the second node, the second electronic message from the second node;
18 wherein:
19 the second electronic message is based on IPsec;
20 the second electronic message is addressed to the third network address;

21 the second electronic message is associated with the second identifier that is
22 different than the first identifier and the third identifier; and
23 the second identifier is generated, based on the third identifier and the
24 specified scheme, by the second node;
25 determining whether the second electronic message is directed to the third node based
26 on the additional value and the second identifier; and
27 when the second electronic message is determined to be directed to the third node,
28 sending the second electronic message to the third node at the third network
29 address.

- 1 47. (Currently Amended) An apparatus as recited in claim 45, wherein the specified
2 scheme is selected from the group consisting of a first scheme that produces a fixed
3 length output, a second scheme that includes a hash algorithm, and a third scheme that
4 includes a Message Digest 49 5 one-way hash function.
- 1 48. (Previously Presented) An apparatus as recited in claim 45, wherein:
2 the value is a hash value;
3 the second identifier is based at least in part on the hash value;
4 the hash value is comprised of a first plurality of bytes;
5 the second identifier is comprised of a second plurality of bytes;
6 a last pair of bytes of the second plurality of bytes is a first pair of bytes of the first
7 plurality of bytes; and
8 the instructions for determining whether the second electronic message is directed to
9 the first node further comprises one or more stored instructions which, when
10 executed by the processor, cause the processor to carry out the steps of:
11 comparing the last pair of bytes of the second identifier to the first pair of
12 bytes of the hash value; and
13 when the last pair of bytes of the second identifier match the first pair of bytes
14 of the hash value, determining that the second electronic message is
15 directed to the first node.

1 49. (Currently Amended) An apparatus as recited in claim 45, wherein:
2 the first node is an IPsec originator node;
3 the second node is an IPsec responder node;
4 the first identifier is a first IPsec security parameter index;
5 the second identifier is a second IPsec security parameter index;
6 the apparatus employs a feature selected from the group consisting of network address
7 translation (NAT), dynamic address NAT, and network address port
8 translation (NAPT);
9 and the apparatus further comprises one or more stored instructions which, when
10 executed by the processor, cause the processor to carry out the steps of:
11 creating and storing a mapping between the value and the first IPsec SPI;
12 security parameter index;
13 creating an association between the value and the first IPsec SPI; identifier;
14 and
15 storing the association in a translation table.

1 50. (Previously Presented) An apparatus as recited in claim 45, wherein the first
2 electronic message and the second electronic message are both based on an IPsec
3 feature selected from the group consisting of IPsec tunnel mode and IPsec
4 Encapsulation Security Payload.

1 51. (Previously Presented) An apparatus as recited in claim 45, further comprising one or
2 more stored instructions which, when executed by the processor, cause the processor
3 to carry out the steps of:
4 when the second electronic message is determined to be directed to the first node,
5 creating an association between the first network address and the second
6 identifier;
7 storing the association in a table;
8 receiving a third electronic message from the second node, wherein the third
9 electronic message is based on IPsec and is associated with the second
10 identifier; and

11 determining that the third electronic message is directed to the first node based on the
12 association.

1 52. (Currently Amended) An apparatus as recited in claim 45, further comprising one or
2 more stored instructions which, when executed by the processor, cause the processor
3 to carry out the steps of:

4 receiving a third electronic from the second node, wherein:
5 the third electronic message is based on IPsec;
6 the third electronic message is addressed to the specified network address;
7 the third electronic message is associated with a third identifier that is
8 different than both the first identifier and the second identifier;
9 the third identifier is a third IPsec SPI; and
10 the third identifier is generated, based on the first identifier and the specified
11 scheme, by the second node;
12 determining whether the third electronic message is directed to the first node based on
13 the value and the third identifier; and
14 when the third electronic message is determined to be directed to the first node,
15 sending the third electronic message to the first node at the first network
16 address.

1 53. (Previously Presented) An apparatus as recited in claim 45, wherein the value is
2 generated before the second electronic message is received.

1 54. (Previously Presented) An apparatus as recited in claim 45, wherein the value is
2 generated after the second electronic message is received.